

IN THE CLAIMS:

Please AMEND claims 1-35 as shown below.

1. (Currently Amended) A method for providing secure access to a packet data network, said method comprising:

- a)——receiving a message from a terminal device, connected to said packet data network;
- b)——deriving a first source information from said message;
- c)——deriving a second source information;
- d)——comparing said first source information and second source information; and
- e)——initiating a protection processing based on ~~the~~ a result of said comparing ~~step~~.

2. (Currently Amended) A method for providing secure access to a packet data network, said method comprising:

- f)——receiving a message from a terminal device, connected to said packet data network;
- g)——deriving a first source information from said message;
- h)——deriving a second source information;
- i)——comparing said first source information and second source information; and
- j)——initiating a protection processing based on ~~the~~ a result of said comparing ~~step~~.

3. (Currently Amended) A method according to claim 1, wherein said second source information is a source address information derived from a packet data unit ~~used for conveying~~configured to convey said message, or from a security association set up between said terminal device and said packet data network.

4. (Currently Amended) A method according to claim 1, wherein said protection processing comprises a processing for dropping said message if the result of said comparing ~~step leads to the result is~~ that said first source information and said second source information do not indicate the same location.

5. (Currently Amended) A method according to claim 1, wherein said protection processing comprises a processing for dropping said message if said comparing ~~step~~ leads to the result that said first source information and said second source information do not match.

6. (Currently Amended) A method according to claim 1, wherein said first source information is an ~~IP~~internet protocol address.

7. (Currently Amended) A method according to claim 6, wherein said message is a SIP session initiation protocol message.

8. (Currently Amended) A method according to claim 1, wherein said second source information is at least a part of an ~~IP~~internet protocol source address of an ~~IP~~internet protocol datagram.

9. (Currently Amended) A method according to claim 1, wherein said second source information is at least a part of an ~~IP~~internet protocol source address of an ~~IP~~internet protocol datagram.

10. (Currently Amended) A method according to claim 3, wherein said second source information is an internet protocol ~~IP~~-address bound to an integrity key of said security association.

11. (Currently Amended) A method according to claim 10, wherein said ~~IP~~internet protocol address is stored in a database of a proxy server ~~(30) provided for routing~~configured to route said message to said packet data network.

12. (Currently Amended) A method according to claim 10, wherein said message is conveyed using a ~~SIP~~session initiation protocol -level protection function.

13. (Currently Amended) A network element for providing secure access to a packet data network, said network element comprising:

a)——receiving means for receiving a message from a terminal device connected to said network element;

b)——deriving means for deriving a first source information from said message, and for deriving a second source information;

e)——comparing means for comparing said first source information and second source information; and

d)——protecting means for initiating a protection processing based on ~~the~~ a comparing result of said comparing means.

14. (Currently Amended) A network element according to claim 13, wherein said deriving means is ~~arranged for deriving~~ configured to derive said second source information from a packet data unit ~~used for conveying~~ configured to derive said message or from a security association set up between said terminal device and said network element.

15. (Currently Amended) A network element according to claim 13, wherein said deriving means is ~~arranged for deriving~~ configured to derive said first source information from a header portion of said message.

16. (Currently Amended) A network element according to ~~any one of claims 13~~ claim 13, wherein said protecting means ~~are arranged~~ is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate ~~the~~ a same location.

17. (Currently Amended) A network element according to ~~any one of claims 13~~ claim 13, wherein said protecting means ~~are arranged~~ is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not match.

18. (Currently Amended) A network element according to ~~any one of claims 13~~ claim 13, wherein said deriving means ~~are arranged for reading~~ is configured to read said second source information from a database provided at said network element.

19. (Currently Amended) A network element according to ~~any one of claims 13~~ claim 13, wherein said deriving means ~~are arranged for deriving~~ is configured to derive said second source information by extracting an ~~IP~~ internet protocol source address from an ~~IP~~ internet protocol ~~diagram~~ datagram.

20. (Currently Amended) A network element according to ~~any of claims 13~~, wherein said network element is a proxy server.

21. (Currently Amended) A network element according to claim 20, wherein said proxy server is a ~~P-CSCF~~ proxy call state control function of an ~~IP~~ internet protocol ~~Mobility~~ mobility ~~Subsystem~~ subsystem.

22. (Currently Amended) A method according to claim 2, wherein said second source information is a source address information derived from a packet data unit ~~used for conveying~~configured to convey said message, or from a security association set up between said terminal device and said packet data network.

23. (Currently Amended) A method according to claim ~~22~~2, wherein said protection processing comprises a processing for dropping said message if the result of said comparing step leads to the result is that said first source information and said second source information do not indicate the same location.

24. (Currently Amended) A method according to claim 23, wherein said protection processing comprises a processing for dropping said message if the result of said comparing step leads to the result is that said first source information and said second source information do not match.

25. (Currently Amended) A method according to claim ~~24~~2, wherein said first source information is an ~~IP~~internet protocol address.

26. (Currently Amended) A method according to claim ~~25~~2, wherein said message is a ~~SIP~~session initiation protocol message.

27. (Currently Amended) A method according to claim ~~26~~2, wherein said second source information is at least a part of an ~~IP~~internet protocol source address of an ~~IP~~internet protocol datagram.

28. (Currently Amended) A method according to claim ~~11~~2, wherein said message is conveyed using a ~~SIP~~session initiation protocol-level protection function.

29. (Currently Amended) A network element according to claim 14, wherein said deriving means is ~~arranged~~configured for deriving to derive said first source information from a header portion of said message.

30. (Currently Amended) A network element according to ~~any one of~~ claims ~~29~~14, wherein said protecting means ~~are~~is arranged~~configured~~ to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate the same location.

31. (Currently Amended) A network element according to ~~any one of~~ claims ~~30~~14, wherein said protecting means ~~are arranged~~is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not match.

32. (Currently Amended) A network element according to ~~any one of~~ claims 3114, wherein said deriving means ~~are arranged for reading~~ is configured to read said second source information from a database provided at said network element.

33. (Currently Amended) A network element according to ~~any one of~~ claims 3214, wherein said deriving means ~~is are arranged for deriving~~ is configured to derive said second source information by extracting an ~~IP~~ internet protocol source address from an ~~IP~~ internet protocol datagram.

34. (Currently Amended) A network element according to ~~any one of~~ claims 3314, wherein said network element is a proxy server.

35. (Currently Amended) A network element according to claim 34, wherein said proxy server is a ~~P-CSCF~~ proxy call state control function of an ~~IP~~ internet protocol ~~Mobility Subsystem~~ subsystem.